Chief Information Officer's Section
Office of the Governor
State of Utah

September 9, 2002

Virus Detection and Removal Policy

Policy Objectives and Scope: This policy is to define common terms relating to computer viruses, define a standard level of virus protection as well as define product requirements.

Definitions:

Computer: For the purposes of this document, a computer will be interpreted to mean an electronic device capable of both connecting to a network and running anti-virus software.

Infection: When a virus, worm, Trojan horse, or variant successfully installs on a host and executes according to its design, causing network or host degradation, damage or otherwise interfering with normal operations.

Trojan Horse: An independent program that appears to perform a useful function while hiding unauthorized executable code that performs unauthorized functions while the user is attempting to execute the program according to its advertised function (including usurping the privileges of the user or compromising confidential information.

Virus: Program fragment that reproduces by attaching itself to another program. It is designed for malicious and, or mischievous purposes and when functioning properly degrades performance on the host computer, the network, consuming system resources or damaging, altering or deleting files on the host. Human interaction triggers virus activity, viruses do not propagate without it. For purposes of this document, the term virus will also include worms, Trojan Horses and other malicious software.

Virus Removal Software: Software designed to detect virulent activity on the host computer or network detect changes in critical configuration, environment, system, or executable files and respond by disabling or removing the perpetrating virus.

Worm: An independent program that reproduces by copying itself from one system to another, primarily targeting networks to slow or even shut them down. Unlike viruses, worms do not require human interaction to propagate.

Message Transfer Agent: Service capable of accepting, storing and forwarding electronic communications data. Including but not limited to SMTP (Simple Mail Transfer Protocol), Internet Messaging Gateways, and instant messaging.

All computers should run anti-virus software: Any State of Utah-owned computer will run current anti-virus software that complies with State software standards. Anti-virus software will be managed by the agency LAN (Local Area Network) administration team under the supervision of administrators knowledgeable in networking, computing devices, email and operating PC Servers. Updates will be installed on devices as often as applicable. An Agency designee working within the guidelines of the established policy shall develop a plan to implement a virus protection program that may be subject to audit.

Electronic Messaging: All State message transfer agents that store files to physical media shall be configured to scan messages, including attachments, for known virus descriptions. State

Agencies will train users regarding potentially dangerous electronic communications, such as responding appropriately to virus alerts.

Response: When a virus is detected, the user shall follow agency incident response procedures.

Product Requirements: Any virus detection product State Agencies implement must provide: continuous virus protection, on demand virus scanning of computers, file quarantine/removal, the ability to prevent users from disabling its function, and automatic virus update functionality.

References:

Interim Date: September 9, 2002
Organization Sponsoring the Standard: ITS, State Information Security Committee (SISC)
State Technical Architect Approval Date: Pending
CIO Approval Date: Pending
ITPSC Presentation Date: 6/27/02 for comment; for approval 9/26/02
Author(s): Rick Gee (ITS), SISC (State Information Security Committee)
Related Documents: State Information Security Policy, State Network Access Policy